USC: Project Proposals

Contents

Name

Unified Secure Channel

Repo Name

usc

Description

In enterprise networks, more and more controller and network management systems are being deployed remotely, such as in the cloud. Additionally, enterprise networks are becoming more heterogeneous - branch, IoT, wireless (including cloud access control). Enterprise customers want a converged network controller and management system solution.

Typical Future Enterprise Networks

blocked URL

Use Cases

Use case 1: Call Home

Network edge initiates the communication to the controller (NMS)

Scenario:

The network edge may be deployed behind a NAT or a firewall, thus the initiation of the session between the controller and network edge has to be from the network edge side; otherwise NAT/FW may drop the session setup request from controller side due to lack of proper states.

Challenges:

- Not all existing protocols provide call home mechanism, such as telnet, vnc, snmp etc.;
- Future network service protocols are mandatorily required to provide call home mechanism if it's server side is on devices.

blocked URL

Use case 2: Two-way authentication

Scenario:

Rogue controller may behave as normal controller and respond to devices' connection request;

Challenges:

- Some existing protocols don't provide solid two-way authentication, such as CAPWAP, SNMP etc.;
- The network edge should also authenticate the controller for its following management and service provisioning.

blocked URL

Use case 3: Unified channel and single-point authentication

Scenario:

Multi-protocol connections between network edge and controller:

-
  - Set up and maintain connections for each protocol;
  - Provide different authentication and security mechanism;

Challenges:

- Various connections to handle, secure channel cannot be reused.
- No consistent and trusted security guarantee;
- Repetitious authentication between a single device and controller

blocked URL

Solution

A unified secure channel for management and service provisioning

blocked URL

Architecture

blocked URL

Scope

Build a unified secure communication tunnel between network element and controller

1. Create a secure channel

1.1 Allow two-way initiation: Initiate the setup from either one of network element or Controller

1.2 Allow two-way authentication

2. Create a generic mechanism to support various communication protocols

2.1 Invisible to protocols carried

2.2 Multiple protocols share the same tunnel

Resources Committed (developers committed to working)

- Helen Chen helen.chen@huawei.com
- Jinzhu Duan duanjinzhu@huawei.com
- Xin Chang xin.chang@huawei.com
- George Zhao george.y.zhao@huawei.com
- An Ho an.ho@huawei.com
- Victor Xu s.xu@huawei.com
- Yan Zhuang zhangyan.zhang@huawei.com

Initial Committers

- Helen Chen helen.chen@huawei.com Username: helenc878
- Jinzhu Duan duanjinzhu@huawei.com Username: djz
- Xin Chang xin.chang@huawei.com Username: XChang
- George Zhao george.y.zhao@huawei.com Username: gzhao
- An Ho an.ho@huawei.com Username: Anipbu
- Victor Xu s.xu@huawei.com Usernmae: Victorxu
- Yan Zhuang zhuangyan.zhuang@huawei.com Username: Yan

Vendor Neutral

- No vendor package names in code
- No vendor branding present in code or output of build
- No vendor branding present in documentation

Meets Board Policy (including IPR)

Reference

File:Odl-usc-2014 11 20.pdf